UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

BELPOINTE SLEEPOVATION INVESTMENT, LP, individually on behalf of itself and all others similarly situated, Plaintiff, v. BOOZ ALLEN HAMILTON, INC. Defendant.	Case No._____ **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Belpointe Sleepovation Investment, LP (hereinafter "Plaintiff"), individually and on behalf of all others similarly situated, brings this action against Defendant Booz Allen Hamilton, Inc. ("Booz Allen" or "Defendant").

NATURE OF THE ACTION

1. This is a class action lawsuit arising from Booz Allen's willful, knowing, and negligent failure to establish basic information security protocols, enabling its own employee to unlawfully access and disseminate the confidential Internal Revenue Service ("IRS") tax return data of Plaintiff and tens of thousands of proposed class members.

2. Booz Allen has made billions of dollars from American taxpayers through its contracts with the Department of the Treasury and the IRS. As a government vendor, Booz Allen accessed and reviewed troves of confidential taxpayer data, including tax returns and return information.

3. Although it was keenly aware of the amount of confidential data it had access to—and the ramifications for allowing this data to remain unprotected—Booz Allen allowed its own employee to illegally access and disclose confidential tax returns and return information. From

2018 through 2021, Booz Allen employee Charles "Chaz" Littlejohn used his position at Booz Allen to access, collect and disseminate the tax returns and/or return information of tens of thousands of American taxpayers' information, including Plaintiff's data.

4. Employee Littlejohn used his Booz Allen hardware and credentials to collect the information, upload the information to a private website, and disclose unknown quantities of this data to the media, including to major publications like ProPublica and the New York Times. These media outlets then used the data to publish articles based on the confidential tax filings. Both outlets have published numerous articles on taxpayers using this confidential data.[1] Littlejohn eventually pleaded guilty to a violation of 26 U.S.C. § 7213(a)(1) for unlawful disclosure of confidential tax return information.

5. In 2024, the IRS sent two rounds of notices to impacted victims of the breach alerting them that their data had been accessed and/or disclosed. The first notice was sent to approximately 70,000 taxpayers, and the second notice is expected to reach over a hundred thousand potentially impacted victims.

6. To date, Booz Allen has taken no responsibility for its role in the breach, and attempts to lay the institutional blame solely at the feet of the IRS—stating in a five-sentence press release that its own employee's "actions were those of a rogue actor hiding his misconduct on

[1] *See, e.g.*, New York Times, *Trump's Taxes Show Chronic Losses and Years of Income Tax Avoidance,* Sept. 27, 2020, https://www.nytimes.com/interactive/2020/09/27/us/donald-trump-taxes.html; ProPublica, *These Real Estate and Oil Tycoons Avoided Paying Taxes for Years*, PROPUBLICA, December 7, 2021, https://www.propublica.org/article/these-real-estate-and-oil-tycoons-used-paper-losses-to-avoid-paying-taxes-for-years; ProPublica, *If You're Getting a W-2, You're a Sucker*, PROPUBLICA, April 15, 2022, https://www.propublica.org/article/if-youre-getting-a-w-2-youre-a-sucker; ProPublica, *How Billionaires Have Sidestepped a Tax Aimed at the Rich*, PROPUBLICA, December 18, 2024, https://www.propublica.org/article/billionaires-net-investment-income-tax; ProPublica, *The Secret IRS Files: Trove of Never-Before-Seen Records Reveal How the Wealthiest Avoid Income Tax*, PROPUBLICA, June 8, 2021.

government systems."[2] But by any measure, Booz Allen is responsible for the actions of its employee. This responsibility is magnified by the fact that Booz Allen was awarded billions of dollars in contracts for government information security, in no small part owing to its outward promises to provide purportedly "best-in-class" solutions to federal agencies including the IRS.

7. Booz Allen's shirking of responsibility for this historic breach cannot continue, and it must be held to account for its role in the access and dissemination of the confidential data of hundreds of thousands of taxpayers, including Plaintiff's and putative Class members'.

THE PARTIES

8. Plaintiff Belpointe Sleepovation Investment, LP is a Limited Partnership organized in the state of Connecticut with its principal place of business in the state of Connecticut. In December of 2024, Plaintiff received a letter from the IRS notifying it that Charles Littlejohn was charged in connection with unauthorized disclosure of Plaintiff's tax return or return information, in violation of 26 U.S.C. § 7431. A true and correct copy of the letter is attached as **Exhibit 1**.

9. Defendant Booz Allen Hamilton, Inc. is an American government and military contractor. Booz Allen is incorporated under Delaware law and headquartered in Virginia. The company provides consulting, analysis, and engineering services to public and private-sector organizations and nonprofits, including the Department of the Treasury and Internal Revenue Service. Booz Allen had yearly revenue of $9.3 billion for the month ended March 31, 2023.

10. Defendant Booz Allen employed Littlejohn at various periods from 2008-2021. Through the conduct of its long-time employee, Littlejohn, Booz Allen unlawfully accessed IRS

[2] Press Release, *Statement Regarding Unauthorized Disclosure of Tax Returns Matter*, May 1, 2024, https://www.boozallen.com/menu/media-center/q1-2025/tax-returns-matter-statement.html

systems and databases that contained confidential tax return information of thousands of American taxpayers, including Plaintiff and the proposed class. On information and belief, Littlejohn worked for Booz Allen in Lanham, Maryland.

JURISDICTION AND VENUE

11. This Court has subject-matter jurisdiction pursuant to 28 U.S.C. § 1332(d)(2)(a) because this case is a class action where the aggregate claims of all members of the proposed class are in excess of $5,000,000.00, exclusive of interests and costs, there are over 100 members of the proposed class, and Plaintiff, as well as most members of the proposed class, are citizens of states different from Defendant. In addition, the Court has subject-matter jurisdiction pursuant to 26 U.S.C. § 7431(a)(2), which authorizes suit in a district court of the United States for the unauthorized disclosure or inspection of tax return or return information by a person who is not an employee of the United States.

12. The Court has personal jurisdiction over Defendant because Defendant has purposefully availed itself of the laws and benefits of doing business in this State, Plaintiff's claims arise out of Defendant's activities in the forum, and a substantial portion of events giving rise to Plaintiff's claims occurred in this District.

13. Venue is proper in this District because a substantial part of the events, omissions, and acts giving rise to the claims herein occurred in this District.

BACKGROUND

A. Booz Allen Profits Handsomely from its Work on Taxpayer Data Security

14. Booz Allen touts itself as having "an established track record of more than 25 years as a strategic mission partner supporting the IRS," with "deep understanding" of IRS

systems.[3] This purported understanding has led to billions in government contracts.

15. Booz Allen has been the recipient of multiple government contracts to enhance the information security and cybersecurity framework of the federal government.

16. In its 2018 Impact Report, Booz Allen advertised its service to the IRS as "Transforming the Taxpayer Experience." In this overview, it specifically highlighted its implementation of "Secure Authentication and Authorization," which it characterized as "[i]mproved access while detecting fraud by highlighting *abnormal user behavior* and suspicious activity."[4]

17. In February 2018, Booz Allen was awarded a $621 million contract to develop the Department of Homeland Security's Continuous Diagnostics and Mitigation ("CDM") program, a government-wide cybersecurity effort to monitor and protect federal networks across agencies (including the IRS).

18. As described by Booz Allen, "DHS chose Booz Allen for the two largest of six competed contracts. We were tapped to provide support for 13 government agencies representing 123 entities with diverse and dynamic missions, from the U.S. Internal Revenue Service (IRS) to the National Aeronautics and Space Administration (NASA). The request was a first and the largest government cybersecurity initiative to date: apply state-of-the-art technology to decades-old infrastructure, with zero impact to agency mission and business operations—and do it at record scale, precision, and speed."[5]

---

[3] Press Release, June 27, 2023, https://www.boozallen.com/menu/media-center/q1-2024/booz-allen-wins-position-on-irs-edos-contract.html

[4] 2018 Impact Report, *The Art and Science of Transformation*, available at https://www.boozallen.com/e/insight/blog/transforming-the-taxpayer-experience.html at 7 (emphasis added).

[5] Case Study, *CDM Cybersecurity Across Federal Agencies*, https://www.boozallen.com/s/insight/thought-leadership/cdm-cybersecurity-across-federal-agencies.html

19. According to its "case study," Booz Allen's "solution included comprehensive plans, meticulous technical architectures and blueprints, best-in-class commercial off-the-shelf solutions, and strategic partnerships with leading industry vendors. We identified and addressed risks across the agency—including operational assets and devices added by internal groups without formal approval (i.e., shadow-IT), to remediate critical security gaps and weaknesses."[6]

20. In August, Booz Allen was awarded another $1.03 billion contract from the same program. DHS, in partnership with the General Services Administration (GSA) Federal Systems Integration and Management Center (FEDSIM), selected Booz Allen as the prime contractor under CDM Dynamic and Evolving Federal Enterprise Network Defense (DEFEND) Program for Group D. At the time, the contract was the largest federal task order and the second-largest cybersecurity task order in Booz Allen's history.

21. According to its case study, "Booz Allen designed and implemented an integrated approach to fulfill the program's five program tasks. Our work revolves around implementing new capabilities, sustaining the data integration layer and dashboard systems, providing expanded agency services and critical incident support, and delivering proactive project management support. In addition to benefiting from DHS' investments, agencies can leverage and apply customized cyber services to address their unique priorities and requirements."[7]

22. Booz Allen further describes CDM DEFEND as offering "integrated solutions and services across four focused capabilities:"

- Asset management: Locate and categorize unauthorized devices and inventory installed software; verify and validate security settings; detect security vulnerabilities;
- Identity and access management: Secure access to needed information, enforce multi-factor authentication, update credentials, and monitor network and system behavior;

[6] *Id.*
[7] *Id.*

- Network security management: Identify and prioritize alerts on changes to security thresholds, monitor traffic, scan custom applications, and identify and report vulnerabilities;
- Data protection management: Segment networks and quarantine devices, manage digital rights to protect devices regardless of location, and protect sensitive information.[8]

23. Booz Allen touted that "[o]ur team deployed CDM capabilities rapidly, helping agencies resolve critical security vulnerabilities within weeks. We then leveraged our proven deployment and integration approaches on other federal organizations, using an agile process to achieve operating capability for all 13 agencies."

24. In June 2023, Booz Allen won a position on the IRS Enterprise Development Operations Services (EDOS) contract, with a ceiling value of $2.6 billion. In its EDOS contract, Booz Allen will "support[] the IRS's applications development portfolio to modernize mission-critical applications efficiently and cost-effectively, while implementing annual tax season legislative requirements."[9]

25. Through these and other agreements, Booz Allen performed a plethora of information security, cybersecurity, IT, and tax administration services for the IRS.

26. Booz Allen, through its employees, had access to IRS systems containing the tax returns and return information of Plaintiff and other American taxpayers.

B. Booz Allen's Prior Information Security Failures

27. The exposure of Plaintiff's and Class members' confidential tax information by and through the actions of Booz Allen's employee Littlejohn was not the first time Booz Allen allowed an information security incident to impact the American public. While Booz Allen makes

[8] *Id.*

[9] Press Release, *Booz Allen Wins Position on $2.6B IRS EDOS Contract*, June 27, 2023, https://www.boozallen.com/menu/media-center/q1-2024/booz-allen-wins-position-on-irs-edos-contract.html

billions of dollars in government IT contracts for its purported expertise in information security and cybersecurity, it has repeatedly permitted its employees to access, download, and disclose highly confidential government and company data.

28. In July 2011, as part of hacking project "AntiSec," the decentralized movement "Anonymous" stole an assortment of data related to other companies and government networks (including a list of approximately 90,000 military email addresses and unsecured passwords) from a Booz Allen database. Anonymous further claimed to have accessed and deleted four gigabytes of the firm's source code and had reportedly discovered "maps and keys" for various government agencies and federal contractors within the Booz Allen unsecured network.

29. Following the breach, Anonymous publicly posted the group's low opinion of Booz Allen's security: "In [Booz Allen's] line of work you'd expect them to sail the seven proxseas [sic] with a state-of-the-art battleship, right? Well you may be as surprised as we were when we found their vessel being a puny wooden barge," explaining that the group had "infiltrated a server on [Booz Allen's] network that basically had no security measures in place."[10]

30. Booz Allen had been named in a prior Antisec breach earlier in the same year, which Anonymous referenced in its public post: "You would think the words 'Expect Us' would have been enough to prevent another epic security fail, wouldn't you?" Anonymous wrote in its statement. "Well, you'd be wrong. And thanks to the gross incompetence at Booz Allen Hamilton probably all military mersonnel [sic] of the U.S. will now have to change their passwords."

31. The group ended the statement by invoicing Booz Allen Hamilton $310 for its

[10] Andy Greenberg, *Anonymous Hackers Breach Booz Allen Hamilton, Dump 90,000 Military Email Addresses*, FORBES, July 11, 2011, https://www.forbes.com/sites/andygreenberg/2011/07/11/anonymous-hackers-breach-booz-allen-hamilton-dump-90000-military-email-addresses ; *see also* https://thepiratebay.org/description.php?id=6533009.

"security audit."[11]

32. Even after this embarrassing and harmful breach which put Booz Allen on notice of its data security shortcomings, Booz Allen's approach to data security did not improve, and instead resulted in one of the most high-profile breaches in U.S. history.

33. Booz Allen employee Edward Snowden, a computer systems administrator, began work on IT systems for the National Security Agency (NSA) in 2013. By May of that year, Snowden had used his Booz Allen position in order to download thousands of top-secret security documents, which he leaked to multiple journalists. While he is wanted in the United States on espionage charges, Snowden received citizenship from Russia and cannot be extradited.[12]

34. Yet even after its employee Snowden exfiltrated this sensitive data, Booz Allen still failed to adequately improve its information security protocols and employee trainings, and Booz Allen's breaches of the public trust continued after the Snowden data theft.

35. In a breach that authorities have called the largest theft of classified information in U.S. history, in 2016, authorities arrested Booz Allen computer analyst Harold Martin for stealing approximately 50 terabytes of confidential data from the NSA dating back to 1996. The stolen data included personal details of government employees and "Top Secret" email chains, handwritten notes describing the NSA's classified computer infrastructure, and descriptions of classified technical operations.

36. Martin's work with Booz Allen involved highly classified projects concerning government computer systems and gave him various security clearances that routinely provided him access to top secret information. Martin ultimately pleaded guilty to a federal charge for willful

[11] *Id.*

[12] Washington Post, *Edward Snowden swears allegiance to Russia and receives passport, lawyer says*, December 2, 2022, https://www.washingtonpost.com/world/2022/12/02/edward-snowden-russian-citizenship/

retention of national defense information.[13]

37. Booz Allen's information security failures have not been limited to attacks by hackers or leaks by so-called rogue actors with political or personal motivations. In fact, the company has facilitated the release of top secret data through sheer negligence, with no "hacking" required.

38. In 2017, while the investigation into the Martin data breach was still ongoing, an independent researcher found tens of thousands of files containing sensitive data that that Booz Allen allowed free for unrestricted public download for at least three months. The files were located on a publicly accessible Amazon Web Services server, and included passwords to sensitive government systems, credentials belonging to a senior engineer at Booz Allen, vulnerability reports on government source code, and identities of government contractors with Top Secret clearances. The exposed files concerned the National Geospatial-Intelligence Agency (NGA), the Department of Defense agency that collects and analyzes data gathered by satellites and drones for the U.S. military and intelligence community.[14]

39. According to the researcher, "[i]nformation that would ordinarily require a Top Secret-level security clearance from the DoD was accessible to anyone looking in the right place; no hacking was required to gain credentials needed for potentially accessing materials of a high classification level. . . . Unprotected by even a password, the plaintext information in the publicly exposed Amazon S3 bucket contained what appear to be the Secure Shell (SSH) keys of a [Booz Allen] engineer, as well as credentials granting administrative access to at least one data center's

[13] Press Release, *Former Government Contractor Pleads Guilty to Federal Charge of Willful Retention of National Defense Information*, March 28, 2019, https://www.justice.gov/opa/pr/former-government-contractor-pleads-guilty-federal-charge-willful-retention-national-defense

[14] Cyberscoop, *Booz Allen Hamilton leaves 60,000 unsecured DOD files on AWS* server, June 1, 2017, https://cyberscoop.com/booz-allen-hamilion-amazon-s3-chris-vickery/

operating system."[15]

40. The researcher's initial attempts to contact Booz Allen "went nowhere" until, a day later, he contacted NGA. It took nine minutes for a response from the intelligence agency and seven more hours for a response from the company.[16]

41. In a statement, Booz Allen said: "Booz Allen takes any allegation of a data breach very seriously, and promptly began an investigation into the accessibility of certain security keys in a cloud environment. . . . As of now, we have found no evidence that any classified information has been compromised as a result of this matter."[17]

42. But according to the researcher, given the files' accessibility, it was "highly likely that malicious actors downloaded and used the publicly exposed data."[18]

43. Still, despite the vulnerabilities of its information security protocols being repeatedly exposed for nearly a decade, Booz Allen failed to ensure its data security practices were sufficient to prevent the exposure of yet more sensitive information.

44. In November 2022, Booz Allen said that one of its staffers, while still employed by the company, downloaded a report containing the personal information of "active employees as of March 29, 2021"—data constituting tens of thousands of other employees' personal information from the company's internal network.[19] The report contained the names, Social Security numbers, compensation, gender, race, ethnicity, date of birth, and U.S. Government security clearance eligibility and status for thousands of Booz Allen employees across the company. Booz Allen said the report containing the personal information was "improperly stored on an

[15] *Id.*
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] TechCrunch, *Booz Allen says former staffer downloaded employees' personal data*, Nov. 18, 2022, https://techcrunch.com/2022/11/18/booz-allen-employee-data-exposed.

internal SharePoint site," but did not say what circumstances led to the discovery of the data, only that it "recently learned" of the staffer's activity.[20]

C. Booz Allen's Unlawful Access and Dissemination of Taxpayer Data

45. Booz Allen's history of unacceptably shoddy information security practices resulted in yet another data breach by one of its own employees—Chaz Littlejohn.

46. Littlejohn worked for Booz Allen from 2008 to 2010, from 2012 to 2013, and then again from 2017 or 2018 through approximately 2021. Littlejohn worked for Booz Allen under contracts Booz Allen had obtained for IRS and/or the Department of the Treasury for work in tax administration, IT services, or cybersecurity work. Littlejohn was enrolled in the company's regular payroll.

47. Littlejohn's review of IRS records was part of Booz Allen's regular business, for work performed under contracts with the IRS or the Department of the Treasury.

48. As Littlejohn's employer, Booz Allen maintained direct control over his daily schedule and activities, instructing him on which work to perform, when to perform it, the manner of the work, and for which IRS projects. Booz Allen maintained direct control over the details of Littlejohn's work, including his time spent analyzing IRS data for tax returns and return information, his project assignments, his performance benchmarks, and his performance reviews.

49. Booz Allen issued Littlejohn a computer, as well as network and database credentials, for performing his IRS data projects.

50. Booz Allen had the ability to monitor Littlejohn's work, but either did not do so or did not do so effectively. From prior experience on his IRS contract work, Littlejohn knew that

[20] Booz Allen, *Consumer Breach Notification* (2022), https://oag.ca.gov/system/files/BAH%20-%20Consumer%20Notification%20Template%20-%20CA.PDF.

as a Booz Allen employee, he could freely access taxpayer data without fear of effective monitoring by his employer.

51. Without restriction or supervision from Booz Allen, Littlejohn began using the IRS databases and systems to extract data about President Trump and other individuals, including Plaintiff and the proposed class members. Littlejohn used the Booz Allen system and its access to the IRS systems and databases to download confidential tax returns and return information.

52. In late 2018, Littlejohn used his Booz Allen credentials to access the tax returns and return information of President Trump and related entities and individuals.

53. Littlejohn queried a database using generalized parameters that would nevertheless collect President Trump's tax return information in the resulting data set. He uploaded this data to a personal, private website to avoid protocols designed to detect and prevent large downloads or uploads from IRS systems. Littlejohn then stored the data in multiple locations, including on personal storage devices, such as his Apple iPod.[21]

54. Between August 2019 and October 2019, Littlejohn disclosed to the New York Times the tax return information associated with President Trump. In the Spring of 2020, Littlejohn stole additional tax return information associated President Trump and provided it to the New York Times. In September 2020, the New York Times published the first of several articles that publicly disclosed information contained President Trump's tax returns.[22]

55. In July and August 2020, Littlejohn separately stole tax returns and return information associated with thousands of the nation's wealthiest individuals. In November 2020, Littlejohn disclosed this tax return information to ProPublica, which has since published nearly 50

[21] Press Release, U.S. TIGTA, February 23, 2024, https://www.tigta.gov/articles/investigations/former-irs-contractor-sentenced-disclosing-tax-return-information

[22] *Id.*

articles using the information provided by Littlejohn.[23]

56. On September 29, 2023, Littlejohn was charged with one count of disclosing tax return information without authorization. On January 29, 2024, Littlejohn was sentenced to five years in prison after pleading guilty to one count of disclosing tax return information without authorization.[24]

57. Littlejohn's plea agreement confirms that he "was authorized, pursuant to 26 U.S.C. § 6103(n), to access vast amounts of unmasked taxpayer data, including taxpayer returns and return information, on IRS databases."[25] Littlejohn had this express authorization to access this data through his employment with Booz Allen.

D. The IRS Victim Notifications

58. While certain high-profile individuals were named in the New York Times and ProPublica articles, until 2024, the vast majority of the taxpayers impacted by the Booz Allen breach were not aware that their confidential data had been compromised.

59. In April 2024, the IRS began informing more than 70,000 individuals and entities impacted by Littlejohn's criminal conduct by mailing brief victim notification letters outlining what Littlejohn had done ("IRS Letter 6613").

60. On May 10, 2024, the IRS issued a statement further explaining its procedures:

> The data set that the IRS received at that point is voluminous and complex, and the IRS has been working with TIGTA to process and analyze this data, including to more fully understand what information, pertaining to what taxpayers, was unlawfully disclosed by Mr. Littlejohn. We are doing this so that we can provide taxpayers with notice of the incident as Section 7431 of the Internal Revenue Code requires, and so that we can take whatever additional steps are warranted to address taxpayer inquiries, interests, and concerns. This has taken some time, which is why we may need to follow up with you through additional correspondence.[26]

---

[23] *Id.*
[24] *Id.*
[25] *United States v. Charles Edward Littlejohn*, 1:23-cr-343 (D.D.C.) (ECF 9, ¶ 3).
[26] IRS Communication on Data Disclosure, May 10, 2024,

61. The IRS provided limited information, noting only that that "If you are receiving this letter, it is our understanding that Mr. Littlejohn unlawfully disclosed information corresponding to your taxpayer identification number maintained on an IRS database. We do not know – at least not at this point – the full scope of the specific information that Mr. Littlejohn unlawfully disclosed. However, a broad set of taxpayer information is maintained in this database."

62. While the IRS noted that it had "seen no indication thus far that any of this information has been disclosed by Mr. Littlejohn to any persons outside of the two news organizations referenced above, or that these news organizations have disclosed this information to any additional persons," it did not affirmatively rule out this additional disclosure.[27]

63. However, even disclosure of Plaintiff's and Class members' most confidential tax information to just these two news organization is a massive breach of Plaintiff's and Class members' privacy—a breach that could have been avoided had Booz Allen taken reasonable actions to ensure its data security practices and protocols were sufficient.

64. In mid-December 2024, the IRS began sending additional notification letters under the title "IRS Notice CP118." These letters contained much of the same information as was included in Letter 6613, with some additional detail outlining the IRS's belief that the information disclosed was "narrow in scope." The individuals and entities receiving the IRS Notice CP118 were not identified previously as victims and thus were not part of the 70,000 or more recipients of IRS Letter 6613.

65. By information and belief, IRS Notice CP118 has been sent to (or is in the process of being sent to) hundreds of thousands of taxpayers.

---

https://www.irs.gov/newsroom/irs-communication-on-data-disclosure.

[27] *Id.*

66. Plaintiff received IRS Notice CP118 in mid-December 2024 (Exhibit 1). Before this time, Plaintiff was not aware that its confidential data had been accessed and/or disclosed.

CLASS ACTION ALLEGATIONS

67. Plaintiff hereby repeats and incorporates by reference each preceding paragraph as though fully set forth herein.

68. Plaintiff seeks to represent a class defined as the following:

> All persons or entities in the United States who received or will receive either IRS Letter 6613 or IRS Notice CP118, indicating that "An Internal Revenue Service (IRS) contractor has been charged with the unauthorized inspection or disclosure of your tax return or return information, between 2018 and 2020."

69. The class definition specifically excludes the following persons or entities: (a) the Defendant named herein; (b) any of the Defendant's parent companies, subsidiaries, and affiliates; (c) any of the Defendant's officers, directors, management, employees, subsidiaries, affiliates or agents; (d) all governmental entities; (e) all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; (f) the judges and chambers staff in this case, as well as any members of their immediate families; and (g) all jurors assigned to this case.

70. Plaintiff reserves the right to modify or amend the definition of the class before the Court determines whether certification is appropriate.

71. Numerosity, Fed. R. Civ. P. 23(a)(1): Plaintiff reasonably believes that the members of the Class number in the tens or hundreds of thousands. The precise number of Class Members and their identities are unknown to Plaintiff at this time but will be determined through discovery. The Class is so numerous and geographically dispersed across the United States that joinder of all members is impracticable.

72. Common Questions Predominate, Fed. R. Civ. P. 23(a)(2) and (b)(3): Numerous questions of law and fact are common to the Class. These common legal and factual questions include, but are not limited to, the following:

(a) Whether Defendant accessed and/or disclosed protected tax information in violation of 26 U.S.C. §§ 6103 and 7431;

(b) Whether Plaintiff and Class Members are entitled to damages;

(c) The measure of Plaintiff and Class Members' damages.

These and other questions of law or fact that are common to the members of the Class predominate over any questions affecting only individual members of the Class. Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claim.

73. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of the claims of other members of the Class. Plaintiff's claim arises from the same common course of conduct giving rise to the claims of the Class, and the relief sought is common to the Class. Plaintiff and the other Class Members were injured by the same unlawful conduct.

74. Adequacy of Representation, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately represent the interests of the Class because Plaintiff received IRS Notice CP118. Plaintiff has no material conflicts with any other members of the Class that would be antagonistic to those of the other members of the Class. Plaintiff seeks no relief that is adverse to the interests of other members of the Class, and the infringement of rights and damages Plaintiff sustained are typical of those of other members of the Class. Furthermore, Plaintiff has retained sophisticated and competent counsel who are experienced in prosecuting class actions, as well as other complex litigation. Plaintiff intends to prosecute this action vigorously.

75. Superiority, Fed. R. Civ. P. 23(b)(3): Class action treatment is a superior method for the fair and efficient adjudication of the controversy in that, among other things, such treatment will permit a large number of similarly situated persons to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of effort and expense that numerous individual actions would engender. The relatively small damages suffered by individual members of the Class compared to the expense and burden of individual prosecution of the claims asserted in this litigation means that, absent a class action, it would not be feasible for members of the Class to seek redress for the violations of law herein alleged. Further, individual joinder of all damaged members of the Class is impractical, and the prosecution of separate actions by individual members of the Class would create the risk of inconsistent or varying adjudications, establishing incompatible standards of conduct for Defendants. Accordingly, the benefits of proceeding through the class mechanism, including providing injured persons with a method of obtaining redress for claims that are not practicable for them to pursue individually, substantially outweigh any difficulties that may arise in management of this class action.

76. This class action is superior to other alternatives for the fair and efficient adjudication of this controversy. Prosecuting the claims pleaded herein as a class action will eliminate the possibility of repetitive litigation. There will be no material difficulty in the management of this action as a class action.

77. The prosecution of separate actions by individual Class Members would create the risk of inconsistent or varying adjudications, establishing incompatible standards of conduct for Defendants.

CLAIMS FOR RELIEF

COUNT I

Violation of 26 U.S.C. §§ 6103 and 7431

78. Plaintiff hereby repeats and incorporates by reference each preceding paragraph as though fully set forth herein.

79. 26 U.S.C. § 7431 provides taxpayers a private right of action for damages against any person who is not an officer or employee of the United States for the knowing or negligent unauthorized inspection or disclosure of tax return information in violation of 26 U.S.C. § 6103.

80. 26 U.S.C. § 6103 provides that tax "[r]eturns and return information shall be confidential" and applies to any "other person (or officer or employee thereof) who has or had access to returns or return information under... subsection (n)" *Id.* § 6103(a)(3).

81. 26 U.S.C. § 6103(n) permits the disclosure of returns and return information to any person "to the extent necessary in connection with the processing, storage, transmission, and reproduction of such returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and the providing of other services, for purposes of tax administration."

82. Booz Allen is a "person. . . who has or had access to [the] returns or return information" of Plaintiff, under 26 U.S.C. § 6103(n), because the Secretary of the Treasury, pursuant to regulations prescribed by the Secretary, disclosed Plaintiff's returns and return information to Booz Allen "to the extent necessary in connection with the processing, storage, transmission, and reproduction of such returns and return information, the programming, maintenance, repair, testing, and procurement of equipment, and the providing of other services, for purposes of tax administration." 26 U.S.C. § 6103(n).

83. The terms "inspected" and "inspection" is defined as "any examination of a return or return information." 26 U.S.C. § 6103(b)(7).

84. "[D]isclosure" is defined as "the making known to any person in any manner whatever a return or return information." 26 U.S.C. § 6103(b)(8).

85. "Return" is defined as "any tax or information return, declaration of estimated tax, or claim for refund required by, or provided for or permitted under, the provisions of this title which is filed with the Secretary by, on behalf of, or with respect to any person, and any amendment or supplement thereto, including supporting schedules, attachments, or lists which are supplemental to, or part of, the return so filed." 26 U.S.C. § 6103(b)(1).

86. "Return information" includes "a taxpayer's identity, the nature, source, or amount of his income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, overassessments, or tax payments, whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing, or any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense." 26 U.S.C. § 6103(b)(2)(A).

87. Booz Allen violated 26 U.S.C. § 6103 from 2018–2021 by inspecting Plaintiff's and Class Members' confidential tax returns and return information, using Booz Allen's hardware and network access to wrongfully inspect data on IRS systems and databases.

88. Booz Allen further violated 26 U.S.C. § 6103 from 2018–2021 by causing the disclosure of the confidential return information to ProPublica and the New York Times.

89. Booz Allen is a self-described "best-in-class" IT and information security vendor.

This experience, coupled with a history of high-profile data breaches by its own employees prior its employment of Littlejohn, put Booz Allen on notice that a breach of the type committed by Littlejohn was likely to occur again. Accordingly, Booz Allen willfully (or at least negligently) declined to establish appropriate practices and procedures ensure the security and confidentiality of Plaintiff's and Class Members' confidential taxpayer information from the foreseeable unlawful inspections and disclosures.

90. Any unlawful inspections and disclosures by Littlejohn were made within the scope of Littlejohn's employment at Booz Allen.

91. Plaintiff and Class Members are entitled to statutory damages in the amount of $1,000 for each act of unauthorized inspection and disclosure. 26 U.S.C. § 7431(c).

COUNT II

Negligent Supervision

92. Plaintiff hereby repeats and incorporates by reference each preceding paragraph as though fully set forth herein.

93. From 2018–2021, Booz Allen performed IT, cybersecurity, tax administration, and other electronic data services for the IRS under contracts with the Department of the Treasury and/or the IRS. The IRS granted Booz Allen access to its computers, networks, and data storage locations to enable Booz Allen to perform those services. The IRS also afforded Booz Allen access to tax databases. Through access to these systems, the IRS enabled Booz Allen and its employees to search, access, download, and disclose confidential tax returns and tax return information, including that of Plaintiff and Class members.

94. During that time, Booz Allen employed Charles Littlejohn and staffed him on assignments that allowed him access to unmasked taxpayer data through the Booz Allen computer network and its connection to the IRS systems and databases.

95. Booz Allen's employee Littlejohn was incompetent. He was capable of inflicting harm by using his access to confidential tax returns and return information to publicly disclose that information. Littlejohn pursued employment at Booz Allen and work on IRS projects for improper political purposes and to malign Americans, including Plaintiff and other Class members. Littlejohn aimed to use his Booz Allen employment and data access credentials to breach IRS systems, misappropriate confidential the taxpayer data of Plaintiff and Class members, and provide it to journalists for worldwide publication with the intent to cause injury to those taxpayers. Mr. Littlejohn willingly disregarded IRS data security and confidentiality restrictions, and unlawfully used his access to IRS data for improper political purposes. He further exploited this access to damage the reputations and businesses of taxpayers like Plaintiff and Class members.

96. Booz Allen knew, or by the exercise of diligence and reasonable care should have known of, Littlejohn's incompetence. Booz Allen knew, or by the exercise of diligence and reasonable care should have known of, Littlejohn's ability to inflict harm through public disclosure of the tax returns and return information he accessed through his employment. Booz Allen knew, or by the exercise of diligence and reasonable care should have known, that Littlejohn was capable of inflicting harm through public disclosure of the private information of Plaintiff and Class members. Booz Allen had or should have had knowledge of Littlejohn's conduct or general character which would have caused a prudent employer in these circumstances to have taken action. On information and belief, Littlejohn made known to Booz Allen supervisors and coworkers his extreme political views, his contempt for wealth, and his criticisms of perceived tax advantages used by the wealthy.

97. Booz Allen knew, or by the exercise of diligence and reasonable care should have known, that Littlejohn was improperly searching for, accessing, inspecting, downloading,

exporting, stealing, and disclosing tax returns and return information. Booz Allen is one of the largest government contractors in the world, with 2023 revenue exceeding $10B. Relevant here, Booz Allen received multiple contracts from the Department of Treasury and/or the IRS, *specifically to safeguard* the IRS's cybersecurity, modernize the IRS database, and assist that agency in tax administration.

98. Booz Allen had a duty to American taxpayers, including Plaintiff and Class members, to supervise the activities of employees such as Littlejohn and stop any unauthorized inspection or disclosure of tax returns or return information.

99. Booz Allen controlled Mr. Littlejohn's project work, his hours, his company computer and network access, and his authorization for access to IRS systems and databases. Booz Allen's IT department had the ability and duty to monitor Littlejohn's searches, views, downloads, uploads, and other activities involving the IRS systems, databases, and taxpayer data. Yet Booz Allen either (a) monitored those activities, yet did nothing to stop them, or (b) willingly chose not to monitor those activities. Booz Allen thus breached its duty reasonably to supervise or monitor its employees and stop any unauthorized inspection or disclosure of confidential and sensitive tax returns or return information.

100. Booz Allen negligently permitted its employees, including Charles Littlejohn, to use its computers, computer networks, or credentials to access IRS systems and databases that contained the tax returns and return information of Plaintiff and Class members.

101. Booz Allen negligently permitted its employees, including Charles Littlejohn, unlawfully to inspect Plaintiff's and Class members' confidential tax returns and return information, and then unlawfully to disclose that information publicly to ProPublica and other media outlets.

102. These actions and omissions breached Booz Allen's duty to American taxpayers, including Plaintiff and Class members, to supervise the activities of employees such as Littlejohn and stop any unauthorized inspection or disclosure of tax returns or return information.

103. Plaintiff's and Class members' taxpayer returns and return information are, and are entitled to be, private facts. Booz Allen negligently allowed its employee, Mr. Littlejohn, publicly to disclose the private facts of Plaintiff's and Class members' tax returns and return information, which amounts to an invasion of privacy and violates Plaintiff's and Class members' statutory protections.

104. Plaintiff's and Class members' tax returns and return information are matters the disclosure of which are highly offensive to a reasonable person and are matters that are not of legitimate concern to the public.

105. This public disclosure of Plaintiff's and Class members' tax returns and return information gave publicity to a matter concerning the private life of Plaintiff and Class members.

106. This public disclosure of Plaintiff's and Class members' tax returns and return information by Littlejohn, a Booz Allen employee, caused Plaintiff's and Class members' actual injuries.

107. Booz Allen's negligent supervision of Mr. Littlejohn proximately caused Plaintiff's and Class members' injuries by allowing the public disclosure of their tax returns and return information to major media outlets and, in some cases, to the general public as well.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff requests that the Court enter judgment on its behalf and on behalf of the Class, by adjudging and decreeing as follows:

(a) Determining that this action may be maintained as a class action under Rule

23(a), (b)(2), and (b)(3) of the Federal Rules of Civil Procedure;

(b) Appointing Plaintiff as representative of the Class and the undersigned law firms as Class Counsel, and direct that reasonable notice of this action, as provided by Rule 23(c)(2) of the Federal Rules of Civil Procedure, be given to each and every member of the Class;

(c) Declaring that Defendant's conduct violates the statutes referenced herein;

(d) Finding in favor of Plaintiff and the Class against Defendant on all counts asserted herein;

(e) Awarding the $1,000 for each unauthorized inspection or disclosure of a return or return information, pursuant to 26 U.S.C. § 7431(c)(1)(A);

(d) Awarding Plaintiff and Class Members their costs and expenses incurred in the action, including reasonable attorneys' fees and costs;

(e) Ordering Defendant to pay pre-judgment interest on all amounts awarded; and,

(f) Awarding Plaintiff and members of the Class such other and further relief as the case may require and the Court may deem just and proper under the circumstances.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of all claims asserted in this Complaint that are so triable.

Dated: January 17, 2025

Respectfully submitted,

/s/ James P. Ulwick

James P. Ulwick (D. Md. Bar No. 00536)
KRAMON & GRAHAM, P.A.
750 East Pratt Street, Suite 1100

Baltimore, Maryland 21202
Telephone: (410) 752-6030
julwick@kg-law.com

James J. Pizzirusso (D. Md. Bar No. 20817)
Nicholas Murphy*
Amanda V. Boltax*
HAUSFELD LLP
888 16th Street N.W., Suite 300
Washington, D.C. 20006
T: 202.540.7200
jpizzirusso@hausfeld.com
nmurphy@hausfeld.com
mboltax@hausfeld.com

Steven M. Nathan (D. Md. Bar No. 30618)
HAUSFELD LLP
33 Whitehall Street 14th Floor
New York, New York 10004
T: 646.357.1100
snathan@hausfeld.com

Linda P. Nussbaum
NUSSBAUM LAW GROUP, P.C.
1133 Avenue of the Americas, 31st Floor
New York, NY 10036
Telephone: (917) 438-9102
lnussbaum@nussbaumpc.com

Michele S. Carino
CARINO LAW LLC
42 Eweler Avenue
Floral Park, NY 11001
Telephone: (347) 452-3675
Fax: (929) 262-6896
mcarino@carinolaw.com